

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-229091

(P2004-229091A)

(43) 公開日 平成16年8月12日(2004. 8. 12)

(51) Int. Cl. ⁷	F I	テーマコード (参考)
H04 L 12/56	H04 L 12/56 100A	5K030
H04 L 12/46	H04 L 12/46 E	5K033
	H04 L 12/46 100R	

審査請求 有 請求項の数 15 O L (全 20 頁)

(21) 出願番号	特願2003-16290 (P2003-16290)	(71) 出願人	000003078
(22) 出願日	平成15年1月24日 (2003. 1. 24)		株式会社東芝
			東京都港区芝浦一丁目1番1号
		(74) 代理人	100058479
			弁理士 鈴江 武彦
		(74) 代理人	100091351
			弁理士 河野 哲
		(74) 代理人	100088683
			弁理士 中村 誠
		(74) 代理人	100108855
			弁理士 蔵田 昌俊
		(74) 代理人	100084618
			弁理士 村松 貞男
		(74) 代理人	100092196
			弁理士 橋本 良郎

最終頁に続く

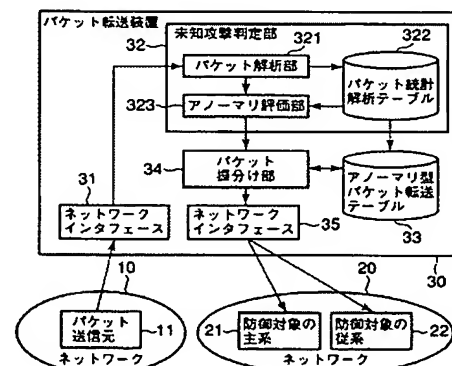
(54) 【発明の名称】 パケット転送システム、パケット転送装置、プログラム及びパケット転送方法

(57) 【要約】

【課題】 攻撃検知の正確性が完全でない場合でも、防御対象の正常なサービスを停止させず、防御対象の致命的な被害から守ることにある。

【解決手段】 同一のサービス機能をもつ主系21及び従系22を備えた冗長構成の防御対象とし、かつ、防御対象にパケットを転送するパケット転送装置30は、防御対象の冗長化構成テーブル33を設け、パケット送信元11から防御対象をアクセスする通信アプリケーションデータを解析し、統計的な評価から攻撃可能性を判定したとき、防御対象の冗長構成を参照し、受信パケットを従系に転送することにより、パケットが攻撃性でないとき、主系とほぼ同様のサービス機能を提供することができる。一方、従系が受け取ったパケットが真に攻撃的なパケットであれば、直接の被害を受けるが、その被害は従系であり、主系は直接の被害を受けなくなるから、未知の攻撃に対して、防御対象の可用性が高い。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

主系及び従系を備えた冗長構成化された防御対象と、
パケット送信元からネットワークを通じて前記防御対象をアクセスするパケットを受信し、この受信されたパケットに関するアプリケーションデータを解析し、統計的な評価のもとに攻撃の可能性を判定し、攻撃可能性の有無に応じて該当受信パケットを前記防御対象の主系と従系とに振分け転送するパケット転送装置とを備えたことを特徴とするパケット転送システム。

【請求項 2】

請求項 1 に記載のパケット転送システムにおいて、
前記防御対象の従系は、前記主系とほぼ同じサービス提供機能を有し、前記攻撃の可能性有りとして受け取ったパケットが真の攻撃でなかった場合には前記主系に代わってサービスを提供することを特徴とするパケット転送システム。

10

【請求項 3】

パケット送信元からネットワークを通じて防御対象をアクセスするパケットを受信し、冗長構成化された主系と従系に振分け転送するパケット転送装置であって、
前記受信パケットに関するアプリケーションデータを解析し、統計的な評価のもとに未知の攻撃の可能性有無を判定する未知攻撃判定手段と、
前記防御対象のネットワークの冗長構成を規定する手段と、
前記未知攻撃判定手段による攻撃可能性有無の判定結果と前記冗長構成とに基づき、前記受信パケットを前記主系と従系とに振分け転送するパケット振分け手段と
を備えたことを特徴とするパケット転送装置。

20

【請求項 4】

主系及び従系を有する防御対象のネットワークの冗長構成が記憶され、パケット送信元からネットワークを通じて防御対象をアクセスするパケットを受信し、同一のサービス提供機能をもつ防御対象の主系と従系に振分け処理するコンピュータに、
前記受信パケットの内容を解析し、統計的な評価に基づく統計情報を取得するパケット解析機能と、この解析機能によって取得された統計情報から攻撃可能性の有無を判定するアノマリ評価機能と、この評価機能の判定結果を受け、前記記憶された冗長構成を参照し、パケット転送先を振分け決定する転送先決定機能と、この決定機能による転送先決定に基づいて前記受信パケットを前記主系又は前記従系に転送するパケット転送機能とを実現させることを特徴とするプログラム。

30

【請求項 5】

パケット送信元からネットワークを通じて防御対象をアクセスするパケットを受信するパケット受信ステップと、
この受信パケットに関するアプリケーションデータを解析し、統計的な評価に基づく統計情報を取得するパケット解析ステップと、
この統計情報から攻撃可能性の有無を判断するアノマリ評価ステップと、
このステップによる攻撃可能性の有無に応じて前記防御対象を構成するほぼ同一機能をもつ主系と従系との何れかの振分けを決定するパケット振分けステップと、
この振分けに従って前記受信パケットを前記主系又は前記従系に転送するパケット転送ステップを有することを特徴とするパケット転送方法。

40

【請求項 6】

ホスト型IDSをもつ主系及び複数のホスト型IDSをもつ従系を備えた冗長構成化された防御対象と、
パケット送信元からネットワークを通じて前記防御対象をアクセスするパケットを受信し、この受信されたパケットに関するアプリケーションデータを解析し、統計的な評価のもとに攻撃の可能性を判定し、攻撃可能性の有無に応じて該当受信パケットを前記防御対象の主系と従系とに振分け転送し、転送先の前記ホスト型IDSをもつ従系側から攻撃検知の通知を受けた場合、次の受信パケットを次のホスト型IDSをもつ従系に切替えて転送

50

可能とするパケット転送装置とを備えたことを特徴とするパケット転送システム。

【請求項 7】

主系及びホスト型IDSをもつ複数の従系を備えた冗長構成化された防御対象と、パケット送信元からネットワークを通じて前記防御対象をアクセスするパケットを受信し、この受信されたパケットに関するアプリケーションデータを解析し、統計的な評価のもとに攻撃の可能性を判定し、攻撃可能性有りの場合に統計的に異常な複数の値域又は前記アプリケーションデータの変数名に従って前記受信パケットを所定のホスト型IDSをもつ従系に転送するパケット転送装置とを備えたことを特徴とするパケット転送システム。

【請求項 8】

パケット送信元からネットワークを通じて防御対象をアクセスするパケットを受信し、冗長構成化された主系とホスト型IDSをもつ複数の従系の何れか1つに振分け転送するパケット転送装置であって、

前記受信パケットに関するアプリケーションデータを解析し、統計的な評価のもとに未知の攻撃の可能性有無を判定する未知攻撃判定手段と、

前記防御対象のネットワークの冗長構成を規定する手段と、

前記未知攻撃判定手段によって攻撃可能性有りの判定結果と前記冗長構成とに基づき、前記受信パケットを所定の従系に振分け転送するパケット振分け手段と、

このパケット転送後、転送先のホスト型IDSをもつ従系側から攻撃検知の通知を受けた場合、転送先従系側が攻撃検知したと認識する従系攻撃検知識別手段と、

この識別手段によって攻撃検知と認識した場合、前記受信パケットを前記冗長構成に従って次の従系に切替えて転送する従系切替手段と

を備えたことを特徴とするパケット転送装置。

【請求項 9】

パケット送信元からネットワークを通じて防御対象をアクセスするパケットを受信し、冗長構成化された主系とホスト型IDSをもつ複数の従系の何れか1つに振分け転送するパケット転送装置であって、

前記受信パケットに関するアプリケーションデータを解析し、統計的な評価のもとに未知の攻撃の可能性有無を判定する未知攻撃判定手段と、

前記防御対象のネットワークの冗長構成を規定する手段と、

前記未知攻撃判定手段によって攻撃可能性有りの判定結果の場合、この判定結果による統計的に異常な複数の値域又は前記アプリケーションデータの変数名に従って前記受信パケットを所定のホスト型IDSをもつ従系に転送するパケット振分け手段と

を備えたことを特徴とするパケット転送装置。

【請求項 10】

主系及びホスト型IDSをもつ複数の従系を有する防御対象のネットワークの冗長構成が記憶され、パケット送信元からネットワークを通じて防御対象をアクセスするパケットを受信し、同一のサービス提供機能をもつ防御対象の主系と従系に振分け処理するコンピュータに、

前記受信パケットの内容を解析し、統計的な評価に基づく統計情報を取得するパケット解析機能と、この解析機能によって取得された統計情報から攻撃可能性の有無を判定するア

ノマリ評価機能と、この評価機能に攻撃可能性有りの判定結果を受け、前記記憶された冗長構成を参照し、何れか1つのホスト型IDSをもつ複数の従系をパケット転送先として決定する転送先決定機能と、この決定機能による転送先決定に基づいて前記受信パケットを前記従系に転送するパケット転送機能と、パケット転送後、転送先のホスト型IDSをもつ従系側から攻撃検知の通知を受けた場合、転送先従系側が攻撃検知したと認識する従系攻撃検知識別機能と、攻撃検知と認識した場合、受信パケットを前記冗長構成に従って次の従系に切替えて転送する従系切替機能と

を備えたことを特徴とするパケット転送装置。

【請求項 11】

パケット送信元からネットワークを通じて防御対象をアクセスするパケットを受信するパ

ケット受信ステップと、
この受信パケットに関するアプリケーションデータを解析し、統計的な評価に基づく統計情報を取得するパケット解析ステップと、
この統計情報から攻撃可能性の有無を判定するアノマリ評価ステップと、
このステップによる攻撃可能性有りの場合、所定の1つの従系に振分けを決定するパケット振分けステップと、
この振分けに従って前記受信パケットを前記所定の1つの従系に転送するパケット転送ステップと、
パケット転送後、転送先のホスト型IDSをもつ従系側から攻撃検知の通知を受けた場合、転送先従系側が攻撃検知したと認識する従系攻撃検知識別ステップと、
攻撃検知と認識した場合、前記冗長構成に従って次の従系に切替える従系切替ステップとを有することを特徴とするパケット転送方法。

10

【請求項12】

請求項8に記載のパケット転送装置において、
前記従系攻撃検知識別手段によって攻撃検知と認識した場合、該当アプリケーションデータをアノマリ評価関数により再評価し、その評価値を閾値とし、統計的に特に異常な値域に組み込むことを特徴とするパケット転送装置。

【請求項13】

主系及び少なくとも1つの従系を備えた冗長構成化された防御対象と、
パケット送信元から送られてくるパケットに関するアプリケーションデータを解析し、統計的な評価のもとに攻撃の可能性を判定し、攻撃可能性の有無に応じて前記パケットを前記防御対象の主系と従系とに振分け転送する複数のパケット転送装置と、
URLと転送先との関係を規定する負荷分散テーブルが設けられ、前記パケット送信元から送られてくるパケットに関するアプリケーションデータに含まれるURLを解読し、当該負荷分散テーブルに規定される前記複数のパケット転送装置及び前記防御対象の何れか1つに受信パケットを送信する負荷分散装置と
を備えたことを特徴とするパケット転送システム。

20

【請求項14】

請求項13に記載するパケット転送システムにおいて、
前記負荷分散装置の負荷分散テーブルに規定するURLと転送先との関係は、変数の有無、変数の数によって定めるものであるパケット転送システム。

30

【請求項15】

主系及び少なくとも1つの従系を備えた冗長構成化された防御対象が設けられ、パケットを当該主系及び前記1つの従系に分散転送するパケット転送方法において、
パケットに関するアプリケーションデータに含まれるURLと転送先との関係が規定され、パケット送信元から送られてくるパケットに関するアプリケーションデータを解読し、この解読結果から得られるURLに基づき、前記複数のパケット転送装置及び前記防御対象の何れか1つに受信パケットを送信する負荷分散ステップを有し、
この負荷分散ステップのもとにパケットを受信した各パケット転送装置が前記請求項5又は請求項11の一連の処理を実行することを特徴とするパケット転送方法。

40

【発明の詳細な説明】**【0001】****【発明の属する技術分野】**

本発明は、ネットワークに対する不正侵入検知技術等に利用されるパケット転送システム、パケット転送装置、プログラム及びパケット転送方法に関する。

【0002】**【従来の技術】**

従来、Webサーバやメールサーバへの不正侵入を早期に検知するために、幾つかの不正侵入検知技術（IDS：Intrusion Detection System）が考えられている。

50

【0003】

その1つは、複数のパケットから得られるアプリケーションデータの統計的解析により、未知の攻撃の可能性を検知する技術が挙げられる。未知の攻撃とは、攻撃の手法が知られておらず、予め記述可能なアプリケーションデータの文字パターンでは検知できない攻撃をいう。

【0004】

この統計的解析を用いた不正侵入検知技術は、図13に示すように防御対象にアクセスしようとするパケットを受信した後、これら複数のパケットから得られるアプリケーションデータの統計的な解析を行い、正常であるか異常であるかを統計的に評価する技術である。この解析によって評価値が統計的に異常な値域に属する場合は攻撃の可能性有りと判定し、警報を発したり、受信パケットを遮断するなどの処置がとられている。

10

【0005】

他の1つは、不正侵入監視部を備えた正規サーバ及び通信セッション引継部を備えたおとりサーバとを設け、不正侵入監視部は、正規サーバと外部端末との間に確立された通信セッションに基づき、パスワードの設定時に間違え回数が基準値を越えた場合、或いはポートスキャンのアクセスを実行した場合、外部端末からの不正侵入と判定し、その不正侵入と判定された通信セッションをおとりサーバの通信セッション引継部に引き継がせることにより、正規サーバを防御する不正侵入検知システムである。

【0006】**【特許文献1】**

特開2002-111727号公報(図2)

20

【0007】**【発明が解決しようとする課題】**

しかしながら、前者の不正侵入検知技術は、アプリケーションデータの統計的解析結果から攻撃の可能性を判定する技術であり、確実に攻撃するとは確定できない未確定の状態にある。その結果、実際には攻撃でないにも拘らず攻撃と誤検知する可能性がある。仮に誤検知した場合にはパケットを遮断してしまうことから、正常なサービスが提供できなくなる。一方、真の攻撃であった場合、パケットを遮断せずに取込むことから、警報を発するが、防御対象が致命的な被害を受けてしまう。

【0008】

一方、後者の不正侵入検知システムは、意図的にセキュリティ性を脆弱させたいいわゆるハニーポットと称するおとりサーバを設け、これを正規のサーバのように見せかけて攻撃をおびき寄せ、攻撃に関する情報を収集するものである。しかし、ハニーポット自体には本来のサービスを提供する機能が備わっておらず、また未知の攻撃の場合には真の攻撃であるか否かが不確実な状態にあるので、前述同様に攻撃でないにも拘らず攻撃と誤検知しおとりサーバに振分けてしまうと、防御対象の正常なサービスを提供できなくなってしまう。

30

本発明は上記事情にかんがみてなされたもので、未知の攻撃に対し、確実な攻撃検知の判定が難しい状態でも、防御対象の正常なサービスを停止させず、かつ、防御対象の致命的な被害から守るパケット転送システム、パケット転送装置、プログラム及びパケット転送方法を提供することを目的とする。

40

【0009】**【課題を解決するための手段】**

上記課題を解決するために、本発明に係わるパケット転送システムは、主系及び従系を備えた冗長構成化された防御対象と、パケット送信元からネットワークを通じて前記防御対象をアクセスするパケットを受信し、この受信されたパケットに関するアプリケーションデータを解析し、統計的な評価のもとに攻撃の可能性を判定し、攻撃可能性の有無に応じて該当採取パケットを前記防御対象の主系と従系とに振分け転送するパケット転送装置とを設けた構成である。

【0010】

50

この発明は以上のような構成とすることにより、統計的な評価のもとに攻撃の可能性が判定されれば、主系と同様のサービス提供機能をもつ従系に振り分けるので、攻撃で無い場合にはサービスを提供することが可能になる。攻撃を受けた場合には、従系であるので、防御対象の主系は致命的な被害を受けることがない。

【0011】

(2) 本発明は、パケット送信元からネットワークを通じて防御対象をアクセスするパケットを受信し、冗長構成化された主系と従系に振分け転送するパケット転送装置であって、
前記受信パケットに関するアプリケーションデータを解析し、統計的な評価のもとに未知の攻撃の可能性有無を判定する未知攻撃判定手段と、前記防御対象のネットワークの冗長構成を規定する手段と、未知攻撃判定手段による攻撃可能性有無の判定結果と冗長構成とに基づき、受信パケットを主系と従系とに振分け転送するパケット振分け手段とを設けたパケット転送装置である。

10

【0012】

この発明においては、受信パケットに関するアプリケーションデータの統計的な解析により評価し、未知の攻撃の可能性があれば、ネットワークの冗長構成から従系に振り分けるので、前記(1)と同様の作用効果を奏する。

【0013】

なお、プログラム及び所定の処理手順に基づく方法によっても以上のような一連の処理を実現することが可能である。

20

【0014】

(3) 本発明に係るパケット転送システムは、ホスト型IDSをもつ主系及び複数のホスト型IDSをもつ従系を備えた冗長構成化された防御対象と、パケット送信元からネットワークを通じて前記防御対象をアクセスするパケットを受信し、この受信されたパケットに関するアプリケーションデータを解析し、統計的な評価のもとに攻撃の可能性を判定し、攻撃可能性の有無に応じて該当受信パケットを前記防御対象の主系と従系とに振分け転送し、転送先の前記ホスト型IDSをもつ従系側から攻撃検知の通知を受けた場合、次のホスト型IDSをもつ従系に切替えてパケットを転送可能とするパケット転送装置とを設けた構成であるので、前記(1)と同様の作用効果を奏する他、従系側から攻撃検知の通知を受けた場合に次の従系に振り分けるので、攻撃を受けた従系を復旧される間でも、次の従系によりサービスを提供することが可能である。

30

【0015】

なお、従系間の振分けについては、攻撃可能性有りの場合に統計的に異常な複数の値域又はアプリケーションデータの変数名に従って振り分けてもよい。

【0016】

(4) 本発明は、パケット送信元からネットワークを通じて防御対象をアクセスするパケットを受信し、冗長構成化された主系とホスト型IDSをもつ複数の従系の何れか1つに振分け転送するパケット転送装置であって、
前記受信パケットに関するアプリケーションデータを解析し、統計的な評価のもとに未知の攻撃の可能性有無を判定する未知攻撃判定手段と、前記防御対象のネットワークの冗長構成を規定する手段と、前記未知攻撃判定手段によって攻撃可能性有りの判定結果と前記冗長構成とに基づき、前記受信したパケットを所定の従系に振分け転送するパケット振分け手段と、このパケット転送後、転送先のホスト型IDSをもつ従系側から攻撃検知の通知を受けた場合、転送先従系側が攻撃検知したと認識する従系攻撃検知識別手段と、この識別手段によって攻撃検知と認識した場合、前記冗長構成に従って次の従系に切替えて受信パケットを転送可能とする従系切替手段とを設けた構成である。

40

【0017】

この発明においても、前記(3)と同様な作用効果を奏することができる。

【0018】

なお、プログラム及び所定の処理手順に基づく方法によっても以上のような一連の処理を

50

実現することが可能である。

【0019】

(5) 本発明に係るパケット転送システムは、主系及び少なくとも1つの従系を備えた冗長構成化された防御対象と、パケット送信元から送られてくるパケットに関するアプリケーションデータを解析し、統計的な評価のもとに攻撃の可能性を判定し、攻撃可能性の有無に応じて前記パケットを前記防御対象の主系と従系とに振り分け転送する複数のパケット転送装置と、URLと転送先との関係を規定する負荷分散テーブルが設けられ、前記パケット送信元から送られてくるパケットに関するアプリケーションデータに含まれるURLを解読し、当該負荷分散テーブルに規定される前記複数のパケット転送装置及び前記防御対象の何れか1つに受信パケットを送信する負荷分散装置とを設けた構成である。

10

【0020】

この発明においては、前記(1)と同様の作用効果を奏する他、負荷分散によりスループットの低下を抑制できる。

【0021】

【発明の実施の形態】

以下、本発明の実施の形態について図面を参照して説明する。

【0022】

(第1の実施の形態)

図1は本発明に係るパケット転送システム及びパケット転送装置の一実施の形態を示す構成図である。

20

【0023】

このパケット転送システムは、インターネットなどの第1のネットワーク10とインターネット、専用ライン、LANその他の伝送ラインなどで構成される第2のネットワーク20と、これらネットワーク10、20間を行き来するパケットを受け取って転送するパケット転送装置30とによって構成されている。

【0024】

第1のネットワーク10は、未知の攻撃を仕掛けると想定される例えばクライアント端末などを含むパケット送信元11が設けられている。パケット送信元11は、未知の攻撃を仕掛けるか否かを無視すれば、図示されていないが複数存在することは言うまでもない。

【0025】

一方、第2のネットワーク20は、主系21と従系22よりなる防御対象が設けられ、防御対象のいわゆる冗長化構成が採用されている。この防御対象としては、例えばWebサーバやFTP(File Transfer Protocol)サーバなどであり、主系21は正しいグループのパケットを受け取るサーバであり、従系22は攻撃の可能性ある怪しいグループのパケットを受け取るサーバであるが、何れも同一のサービス提供機能をもつものであり、異なる機器どうしの場合には冗長構成のとれる機器どうしの組み合わせが好ましい。なお、防御対象の主系21と従系22は、1対1の関係にあるが、1つの主系21に対して複数の従系22、…、又は主系21と従系22がそれぞれ複数存在する構成であってもよい。

30

【0026】

パケット転送装置30は、パケット送信元11から防御対象にアクセスしようとするパケットを受信するネットワークインタフェース31、このインタフェース31により受信されたパケットから未知の攻撃の可能性有無を判定する未知攻撃判定部32、防御対象におけるネットワークの冗長構成を規定するアノマリ型パケット転送テーブル33、この未知攻撃判定部32による判定結果に基づき、パケット転送テーブル33の冗長構成を参照し、パケットの振り分け処理を実行するパケット振り分け部34及び振り分け処理結果に従って受信パケットを主系21a、従系21bの何れかに転送するネットワークインタフェース35が設けられている。

40

【0027】

未知攻撃判定部32は、パケット解析部321、パケット統計解析テーブル322及びア

50

ノーマリ評価部 3 2 3 によって構成されている。パケット解析部 3 2 1 及びパケット統計解析テーブル 3 2 2 は、複数のパケットから構成されるアプリケーションデータを解析し記憶する機能をもつものであり、具体的には、パケット解析部 3 2 1 が複数のパケットを採取し、防御対象で使用されるプロトコルレイヤのアプリケーションデータ（分割された複数のパケットの組み合わせデータ）を構成し、当該プロトコルレイヤによって規定される規則を利用し、文字区分や数値情報等を抽出し解析することにより、図 2 に示すような統計的な評価値 $f(x)$ を算出し、この評価値 $f(x)$ から例えば平均値や分散を計算し、後記する図 4 に示すごとく統計情報としてパケット統計解析テーブル 3 2 2 に記憶する。

【0028】

前記アノーマリ評価部 3 2 3 は、パケット統計解析テーブル 3 2 2 に記憶されたアプリケーションデータの解析結果である統計情報から統計的に正常な値域 y_1 、統計的に異常な値域 y_2 を評価し、正常な値域 y_1 及び異常な値域 y_2 に属する評価結果をパケット振分け部 3 4 に送出する。なお、図示されていないが極めて異常な値域に属する場合は、パケット解析部 3 2 1 又はアノーマリ評価部 3 2 3 でパケットが捨てられ、防御対象へのアクセスを遮断する。

【0029】

パケット振分け部 3 4 は、アノーマリ評価部 3 2 3 からの評価結果に基づき、統計的に正常な値域 y_1 に属するパケットの場合、アノーマリ型パケット転送テーブル 3 3 の冗長構成に基づき、受信パケットを主系 2 1 に振分け、統計的に異常な値域 y_2 に属するパケットの場合、同様の手順に基づいて従系 2 2 に受信パケットを振分ける処理を実行する。ネットワークインタフェース 3 5 は、振分け処理結果に従って主系 2 1 又は従系 2 2 の何れかに受信パケットを転送する。

【0030】

なお、パケット統計解析テーブル 3 2 2 とアノーマリ型パケット転送テーブル 3 3 はそれぞれ個別のテーブルが使用されているが、後記する図 5 に示すように同一のテーブルを区分けして使用してもよい。

【0031】

次に、本発明の第 1 の実施の形態に係わるプログラム及びパケット転送方法について図 3 及び図 4 を参照しながら説明する。図 3 はパケット転送装置 3 0 が CPU で構成されている場合、このパケット転送装置 3 0 には受信パケットを防御対象の主系 2 1 と従系 2 2 とに振分け処理するプログラムを格納するプログラムメモリ 4 1 が接続される。

【0032】

先ず、パケット転送装置 3 0 が動作を開始すると、プログラムメモリ 4 1 に格納されるプログラムを読み出し、適宜なメモリに格納する。この状態において、パケット送信元 1 1 から第 1 のネットワーク 1 0 を通じて防御対象にアクセスしようとするパケットが到来すると、当該パケットをネットワークインタフェース 3 1 にて受信し、パケット解析部 3 2 1 に相当するパケット解析機能 3 2 1 a に渡す（S 1：パケット受信ステップ）。

【0033】

このパケット解析機能 3 2 1 a は、受信したパケットに関し、前述するように防御対象 2 1 で使用されるプロトコルレイヤのアプリケーションデータを構成し、このアプリケーションデータから文字区分や数値情報等を抽出し解析し（S 2）、統計的な評価値 $f(x)$ を算出し、この評価値 $f(x)$ から平均値や分散を求め、統計情報としてパケット統計解析テーブル 3 2 2 に記憶する（S 3）。この S 2、S 3 はパケット解析ステップに相当する。

【0034】

引き続き、パケット転送装置 3 0 は、アノーマリ評価部 3 2 c に相当するアノーマリ評価機能 3 2 3 a を実行する。このアノーマリ評価機能 3 2 3 a は、パケット統計解析テーブル 3 2 2 に記憶された統計情報から統計的に正常な値域 y_1 か統計的に異常な値域 y_2 か、つまり統計的に「アノーマリ」であるか否かを判断する（S 4：アノーマリ評価ステッ

10

20

30

40

50

プ)。ここで、「アリーマリ」とは、過去に防御対象 2 1 にアクセスしたパケットの解析結果（統計情報）を参照し、統計的に異常であると評価されるものを指す。このようなパケットは、完全に攻撃とは言いつれないが、攻撃の可能性があるとは判断される。

【0035】

さらに、パケット転送装置 3 0 は、パケット振分け部 3 4 に相当する転送先決定機能 3 4 a を実行する。この転送先決定機能 3 4 a は、パケットが「アリーマリ」とであると評価された場合、パケット転送テーブル 3 3 の冗長構成を参照し、パケットの転送先を防御対象の従系 2 2 であると決定し（S 5）、またパケットが「アリーマリ」でないと評価された場合、同じくパケット転送テーブル 3 3 の冗長構成からパケットの転送先を防御対象の主系 2 1 であると決定する（S 6：パケット振分けステップ）。

10

【0036】

さらに、パケット転送機能 3 5 a を実行する。このパケット転送機能 3 5 a は、ステップ S 5 によるパケット転送先決定に基づいて受信パケットを防御対象の従系 2 2 に転送し（S 7）、また S 6 によるパケット転送先決定に基づいて受信パケットを防御対象の従系 2 1 に転送する（S 8）。この S 7、S 8 はパケット転送ステップに相当する。

【0037】

従って、以上のような実施の形態であるパケット転送システム、パケット転送装置、プログラム及びパケット転送方法によれば、未知の攻撃の可能性があるとは評価した場合には、防御対象の従系 2 2 に転送するが、この従系 2 2 は、未知の攻撃の可能性がある怪しいパケットを受けもつサーバであるが、主系 2 1 とほぼ同様のサービス機能を有するので、仮にパケットが攻撃無しであれば、主系 2 1 とほぼ同様のサービス機能を提供することができる。一方、従系 2 2 が受け取ったパケットが真に攻撃的なパケットであれば、直接の被害を受けるが、その被害は従系 2 2 であり、主系 2 1 は直接の被害を受けなくなるから、未知の攻撃に対して、防御対象の可用性が高くなる効果を期待できる。

20

【0038】

また、「アリーマリ」と評価されたパケットは、攻撃ではないが、通常のサービスを要求しない可能性もある。例えば攻撃者が攻撃を行う前に、正常な使われ方でないパケットを防御対象に送り付け、当該防御対象からの応答パケットを調べて攻撃の手口を探るフィンガープリンティングという手法を利用する例もある。このような手法を利用したパケットを防御対象の主系 2 1 に転送した場合、主系 2 1 はそのパケット処理が無駄となり、防御対象本来のサービス提供に振り向けられず、処理能力の低下となる。しかし、本発明においては、「アリーマリ」でないと評価されるパケットが従系 2 2 に転送するので、主系 2 1 による無駄処理がなくなり、迅速にサービスを提供することができる。

30

【0039】

なお、前記未知攻撃判定部 3 2 は、様々なプロトコルレイヤを対象とするので、それぞれ防御対象により使用されるプロトコルレイヤに規定されるデータフォーマットに応じた統計解析処理が実施できるようにすることが好ましい。

【0040】

次に、具体的に Web サーバを用いた防御対象に対する未知の攻撃の判断の一例について説明する。

40

【0041】

この Web サーバに対する攻撃の典型的な事例としては、CGI（Common Gateway Interface）に特別なメタキャラクタを伴うスクリプトが挿され、Web サーバが実行されてしまったり、或いは特別に長い文字列を与えることにより CGI にバグを発生させ、Web サーバにバッファオーバーフローなどの誤動作を起こさせるなど、攻撃として成立する事例が非常に多く出回っている。また、攻撃が成立した場合、通常人間が Web ブラウザから入力しないような長いバイナリコードを Web サーバに送り付け、実行させられる例もある。さらに、インターネット上で取り扱う CGI は、日々新たに開発されており、それに伴って未知の脆弱性と未知の攻撃も増え続けている。

【0042】

50

そこで、Webサーバに対する未知の攻撃の可能性を判定する場合においては、CGIに与える変数の値を構成する文字セットを分類分けし、各文字セットごとに統計的な分布から「アノマリ」を評価することが好ましい。

【0043】

以下、各文字セットごとに統計的な分布から「アノマリ」を評価する例について説明する。

【0044】

未知攻撃判定部32の packets 解析部321は、パケット送信元11から防御対象にアクセスするパケットを採取し、複数のパケットのデータからアプリケーションデータを構成する。このアプリケーションデータは、防御対象がWebサーバであるので、HTTP (Hypertext Transfer Protocol) データを構成する。パケット解析部321は、アプリケーションデータであるHTTPデータを、HTTPで規定されるプロトコルに従って解釈し、URL名、CGIの変数名、変数の値、この値に含まれる文字等の文字列区分や数値情報を抽出し、統計的な評価分布から平均値、分散を取得し、パケット統計解析テーブル322に記憶する。

【0045】

図5はWebサーバにアクセスするパケットに関するパケット統計解析テーブル322とアノマリ型パケット転送テーブル33のデータ配列例を示す図である。パケット統計解析テーブル322は、Webサーバにアクセスするアプリケーションデータを解析し、かつ、統計的に解析した統計情報が記憶される。このテーブルの行51は、URL名を記憶するエリアであり、例えばURL名a、URL名b、URL名c、…のように記憶する。一方、テーブルの列52は、URLで示されるものがCGIである場合、CGIに与えられた変数名を記憶するエリアであり、例えば変数名x1、変数名x2、変数名x3、…のように記憶する。但し、WebサーバにアクセスするHTTPデータの中には全く変数が与えられないURLもある。

【0046】

一般に、URL名と変数名は、Webサーバ内では限られた数であるので、防御対象であるWebサーバにアクセスしてくるHTTPデータから学習記憶し、テーブルの行・列に順次記憶しておく。

【0047】

URL名と変数名から参照される個々のセルは、詳しくは統計情報を記憶されるセル53であって、学習段階において蓄積される統計情報が記憶される。つまり、あるURL名bに与えられたある変数名x2に関する値の統計情報が記憶される。このセル53の行54は、値の構成要素を分類分けするものであり、文字セットA、文字セットB、文字セットC、…のように分類分けする。この文字セットA、B、…は、具体的には「数値」、「ASCII (アスキー) 文字」、「メタキャラクタ (プロトコルやスクリプト言語で特殊な意味をもつ文字)」、「その他 (例えばバイナリコード)」などに分類される。このセル53の列55は、値の長さに関する統計情報を記憶するものであって、HTTPがアクセスされる毎に学習段階で図2に示す統計的な評価分布に基づいて平均値56、分散57を再計算し、当該再計算の度に更新される。

【0048】

以上のようにして十分に学習された統計情報に基づき、次のようなアノマリ評価を実施する。すなわち、パケット送信元11から防御対象にアクセスするためにHTTPデータが与えられた場合、このHTTPデータのもとにパケット統計解析テーブル322に該当するURL名と変数名との組が存在するか否かを判断し、存在する場合にはそのセル53内に記憶される統計情報を参照し、値の構成要素である文字セットの各々について、値の長さの平均値56と分散57とに基づいて統計的に異常な値域であるかどうか、すなわちアノマリであるか否かを判定する。この判定処理は、アノマリ評価関数 $f(x_1, x_2, x_3, \dots)$ による値の計算と形式的に同一視できる。

【0049】

そして、評価値が正常値の値域に属するならば防御対象の主系21にパケットを転送し、評価値が異常値の値域に属するならば防御対象の従系222にパケットを転送する。ところで、アノマリ評価関数 $f(x_1, x_2, x_3, \dots)$ による値域からパケットの転送先を決定するが、この決定に際しては、予めURL毎に、アノマリ評価関数 $f(x_1, x_2, x_3, \dots)$ による値域と、それに対するパケット転送先とを規定するアノマリ型パケット転送テーブル33を参照し、主系21か従系22かを決定する。

【0050】

なお、パケット送信元11から与えられるパケットのHTTPデータが一度もアクセスされたことのないURL名と変数名との組、或いは単にURL名だけの場合、その時点でアノマリと判定してもよい。また、WebサーバのCGIによつては、変数名が与えられず値のみが与えられる。このような場合には、パケット統計解析テーブル322は、変数名を考慮した二次元の「表形式」である必要はなく、URL名だけの一次元の「列」で構成されることもある。

【0051】

また、以上の実施の形態では、防御対象が主系21と従系22からなる二重構成であるが、それ以上の多重構成であつてもよい。この場合には、アノマリ型パケット転送テーブル33のアノマリ評価関数 $f(x_1, x_2, x_3, \dots)$ の値域を複数設定し、それに対応したパケット転送先を複数設定することになる。

【0052】

(第2の実施の形態)

図6は本発明に係るパケット転送システムの一実施の形態を示す系統構成図である。なお、このパケット転送システムは、その大部分が図1とほぼ同様な構成であるので、同一部分には同一符号を付し、詳しくは図1及びその関連図の説明に譲る。

【0053】

このパケット転送システムの特に異なるところは、防御対象、パケット転送装置30の一部の構成であるアノマリ型パケット転送テーブル33及びネットワークインタフェース35を含むパケット振分け部34を改良した点にある。

【0054】

防御対象は、複数の従系221, ..., 22Nが設置され、主系21を含むこれら各従系221, ..., 22Nにはそれぞれホスト型IDS23、241, ..., 24Nが設けられている。ここで、ホスト型IDSとは、防御対象のホスト上に適用される実際の攻撃を検知する機能をもったプログラムである。

【0055】

なお、アノマリ評価関数 $f(x_1, x_2, x_3, \dots)$ の値域としては、図7に示すように統計的に正常な値域 y_1 と、統計的に異常な値域 y_2 と、統計的に特に異常な値域 y_3 とがあるが、そのうち統計的に特に異常な値域 y_3 は、通常、パケット解析部321又はパケット振分け部34で遮断されるが、統計的に異常な値域 y_2 については、前述する複数の従系221, ..., 22Nを設けることにより、アノマリ型パケット転送テーブル33は、例えば図8(a)~(c)に示すようにアノマリ評価関数 $f(x_1, x_2, x_3, \dots)$ の値域とパケットの転送先とを関係付ける構成を採用する。

【0056】

同図(a)は、アノマリ評価関数 $f(x_1, x_2, x_3, \dots)$ の値域 y_1, y_2, y_3, \dots のうち、値域 y_2 に対して防御対象の複数の従系221, ..., 22Nを割当てる例である。同図(b)は、アノマリ評価関数 $f(x_1, x_2, x_3, \dots)$ の値域 y_1, y_3 に対してパケット転送先を共通に設定し、アノマリ評価関数 $f(x_1, x_2, x_3, \dots)$ の値域 y_2 については各変数名ごとに防御対象の従系221, ..., 22Nを割当てる例である。また、同図(c)は、統計的に異常な値域 y_2 を複数の値域 y_{21}, \dots, y_{2n} に分け、これら値域 y_{21}, \dots, y_{2n} ごとに従系221, ..., 22Nを割当てる例である。

【0057】

すなわち、未知攻撃判定部 3 2 は、図 8 (a) に示すアノマリ型パケット転送テーブル 3 3 を用いる場合、未知攻撃の可能性ありと評価されたとき、通常、パケット振分け部 3 4 が従系 2 2 1 を転送先と決定し、パケットを転送するが、当該従系 2 2 1 に対応するホスト型 IDS 2 4 1 で本当の攻撃と検知された場合、次に受信されるパケットに対して次の従系 2 2 2 (図示せず) を転送先と決定する。これは従系 2 2 1 を復旧させる間でも、引き続き、他の防御対象の従系 2 2 2 がサービスを提供可能な状態にするためである。また、未知攻撃判定部 3 2 は、図 8 (b)、(c) に示すアノマリ型パケット転送テーブル 3 3 を用いる場合、パケット振分け部 3 4 で決定されるパケット転送先に従ってパケットを転送する。図 8 (b) の場合には、何れかの変数名で攻撃可能性を判定した場合、当該変数名から従系を決定する。図 8 (c) の場合には、何れの値域 y_{21} , ..., y_{2n} で攻撃可能性を判定した場合、ひいては該当値域に基づいて従系をパケット転送先と決定する。

10

【0058】

従って、図 8 (a) ~ (c) のようなアノマリ型パケット転送テーブル 3 3 を構成することにより、より正しい評価を下すことが可能であり、攻撃があった場合にもサービスの継続性を維持することが可能である。

【0059】

次に、本発明における第 2 の実施の形態に係わるプログラム及びパケット転送方法について図 9 及び図 10 を参照しながら説明する。但し、この例は、図 8 (a) に示すアノマリ型パケット転送テーブル 3 3 を用いた例について説明する。

20

【0060】

パケット転送装置 3 0 が CPU で構成されている場合、このパケット転送装置 3 0 には受信パケットを防御対象の主系 2 1 と従系 2 2 1, ..., 2 2 N とに振分け処理するプログラムを格納するプログラムメモリ 5 8 が設けられている。

【0061】

先ず、パケット転送装置 3 0 が動作を開始すると、プログラムメモリ 5 8 に格納されるプログラムを読み出し、プログラムを実行するが、機能的にはパケット解析機能 3 2 1 a、アノマリ評価機能 3 2 3 a、転送先決定機能 3 4 a、パケット転送機能 3 5 a は図 3 と同様であり、またパケット転送処理手順については、図 4 の処理手順 S 1 ~ S 7 と同様であるので、それぞれの図の説明に譲り、以下、異なる部分について説明する。

30

【0062】

すなわち、パケット転送装置 3 0 は、パケット転送機能 3 5 a によってパケットを転送した後 (S 7)、従系攻撃検知識別機能 3 4 b を実行する。この従系攻撃検知識別機能 3 4 b は、パケットを転送した後、転送先の従系例えば 2 2 1 に対応するホスト型 IDS 2 4 1 が攻撃を検知したか否かを判断する (S 1 1)。このホスト型 IDS 2 4 1 は、ネットワークインタフェース 3 5 からパケットを受け取ると、前述するように実際の攻撃であるか否かを検知し、攻撃であると検知するとトリガ情報として例えば SNMP (Simple Network Management Protocol) トラップをパケット転送装置 3 0 に通知する。従って、従系攻撃検知識別機能 3 4 b は、転送先である従系 2 2 1 から攻撃検知の通知を受けると、何れの防御対象上で攻撃を検知したかを識別する (S 1 2)。この S 1 1, S 1 2 は従系攻撃検知識別ステップに相当する。

40

【0063】

引き続き、パケット転送装置 3 0 は従系切替機能 3 5 b を実行する。この従系切替機能 3 5 b は、アノマリ型パケット転送テーブル 3 3 に規定する図 8 (a) から予め定められた順序に従って例えば従系 2 2 2 に切り替え、以降に受信する攻撃可能性あるパケットを転送する (S 1 3: 従系切替ステップ)。

【0064】

なお、アノマリ型パケット転送テーブル 3 3 の構成が図 8 (b)、(c) の場合、パケット振分け部 3 4 又は転送先決定機能 3 4 a は、アノマリ型パケット転送テーブル 3 3 に規定する冗長構成から、統計的に異常な複数レベルの値域 y_{21} , y_{22} , ... または変

50

数名に基づいて決定し、ホスト型IDSをもつ複数の従系221, ..., 22Nの中から1の従系を振分け先とする。

【0065】

従って、以上のような第2の実施の形態によれば、少なくとも防御対象にホスト型IDSをもつ複数の従系221, ..., 22Nを設け、パケット転送装置30は、受信パケットが攻撃可能性有りと評価されたとき、アノマリ型パケット転送テーブル33の規定に従って1つの従系にパケットを転送するが、この転送先従系のホスト型IDSから攻撃検知の通知を受けたとき、予め定める次の従系にパケットを転送するように切替えるので、当該攻撃を受けた従系を復旧させる間にパケットを受信しても、他の従系に振り分けてサービスを提供することが可能となり、防御対象の可用性を高めることができる。

10

【0066】

なお、上記実施の形態は、従系のホスト型IDSから攻撃検知の通知を受けたとき、パケット転送テーブル33の規定に従って次の従系に切替える構成であるが、例えば従系のホスト型IDSから攻撃検知の通知を受けたとき、攻撃検知時のアプリケーションデータをアノマリ評価関数により再評価し、その評価値を閾値とし、統計的に特に異常な値域 y_3 に属させ、パケットを明示的に遮断する学習ルールとしてもよい。すなわち、図7に示すように、アプリケーションデータの解析による統計的な評価値 $f(x)$ に対し、統計的に正常な値域 y_1 と、統計的に異常な値域 y_2 と、従系側のホスト型IDSで攻撃検知とされたデータの評価値を閾値とする統計的に特に異常な値域 y_3 に属させ、攻撃の可能性が高く、かつ、統計的に特に異常な値域に属する場合には明示的にパケットを遮断すれば、攻撃の可能性が高いものに対する防御対象の安全性を向上させることができる。

20

【0067】

(第3の実施の形態)

図11は本発明に係るパケット転送システムの一実施の形態を示す系統構成図である。

【0068】

このパケット転送システムは、パケット送信元11が設けられている第1のネットワーク10と、冗長構成化された主系と1つ又は複数の従系とを備えた防御対象が設けられている第2のネットワーク20と、これらネットワーク10, 20を行き来するパケットを転送するパケット転送装置とが設けられている点は第1、第2の実施の形態と同様である。従って、第2のネットワーク20に設けられる防御対象は、第1、第2の実施の形態と同様な構成であるので、それらの説明に譲り、その具体的な構成は図面から省略している。

30

【0069】

この実施の形態において、特に異なるところは多重化されたパケット転送装置30A, 30Bを設けたこと、また複数のパケット転送装置30A, 30Bとネットワーク20との間にURLスイッチ60を設置する一方、当該URLスイッチ60とネットワーク20間に複数のパケット転送装置30A, 30Bを介さずに直接接続される伝送ライン61を設けたことなどである。なお、パケット転送装置30A, 30Bの構成は、第1、第2の実施の形態と同様な構成であるので、それらの実施の形態の説明に譲り、図面にはパケット統計解析テーブル322A, 322Bだけを記載し、他の具体的な構成は省略する。

【0070】

以上のようにパケット転送装置を多重化構成とした理由は次の通りである。パケット転送装置は、統計解析を行う観点から、アプリケーションデータのURL名のみならず、CGIの変数名、各変数名の値などが必要となり、防御対象のトラフィック量が大きくなり、スループットが十分に出なくなる懸念がある。

40

【0071】

そこで、この実施の形態では、複数のパケット転送装置30A, 30Bを設け、パケット転送装置30Aには図12(b)に示すパケット統計解析テーブル322A、パケット転送装置30Bには図12(c)に示すパケット統計解析テーブル322Bを設けるとともに、複数のパケット転送装置30A, 30Bとネットワーク10との間にURLスイッチ60を設け、負荷の分散を図る構成を採用している。

50

【0072】

このURLスイッチ60は、レイヤ7スイッチとも言われ、一種の負荷分散装置であり、図12(a)に示すように負荷分散テーブル62にURLと負荷分散先とを関係付け、パケットの分散を図る構成である。URLスイッチ60は、例えば専用のハードウェア構成によりアプリケーションデータに含まれるURLを高速に解読し、この解読されたURLのもとに負荷分散テーブル62を参照し、複数のパケット転送装置30A、30B、ネットワーク20のいずれかにパケットを振分ける。

【0073】

さらに、図11に示すパケット転送システムについて詳細に説明する。

【0074】

第1の実施の形態における図5に示すパケット統計解析テーブル322に着目すると、URL名が当該テーブルの行に一意に記憶されている。一方、この実施の形態では、図12に示すようにURL名に基づいてテーブルを複数に分割し、この分割されたテーブル数だけパケット転送装置を設置し、分割されたテーブルを各パケット転送装置に個別に割り当てている。

【0075】

一方、URLスイッチ60における負荷分散テーブル62にはURL名と負荷分散先とを関係付けることにより、アプリケーションデータに含まれるURLに基づき、負荷分散テーブル62から分散先である1つのパケット転送装置を検索し、アプリケーションデータの統計解析処理を実行させることにより、防御対象のURL名の数と、防御対象に対するトラフィック量とが大きくなっても、スループットの低下を抑えるようにする。

【0076】

ところで、多数のURLのうち、特定のURL（例えばURL名g、URL名h、URL名i）は、パケット転送装置による統計解析によって変数が全く与えられないことが明らかな場合、当該URL名を含むアプリケーションデータは、URLスイッチ60からパケット転送装置を経由させずに直接に防御対象が存在するネットワーク20に向けるように、負荷分散テーブル62を変更することが好ましい。

【0077】

そこで、パケット転送装置は、統計的に変数が全く与えられないURLのリストをURLスイッチ60に通知し、当該URL名とともにパケット分散先をネットワーク20の防御対象であることを負荷分散テーブル62に登録する。なお、URLのリストを通知するためのプロトコル手段は、URLスイッチ60が解釈できるものであれば特に問わない。これにより、変数名やその値に関する攻撃の可能性の無いパケットは、アプリケーションデータの統計解析処理と異常性の評価処理が省略されるので、スループットの低下を抑制する効果が得られる。

【0078】

また、パケット転送装置は、統計解析により、与えられる変数の数が比較的多いことが明らかになった場合、同様にURLスイッチ60に通知する。その結果、URLスイッチ60は、以上のようなURL名を含むアプリケーションデータを比較的处理性能の高いパケット転送装置に向けるように負荷分散テーブル62に登録する。これにより、変数の数が比較的多く、統計解析処理と異常性の評価処理の負荷が大きいアプリケーションデータは、処理性能の高いパケット転送装置に処理させる。一方、変数の数が比較的小なく、統計解析処理と異常性の評価処理の負荷が小さいアプリケーションデータは、処理性能の低いパケット転送装置に処理させることにより、全体的にバランスよく負荷を分散でき、スループットの低下を抑制できる効果を奏する。

【0079】

なお、本願発明は、上記実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々変形して実施できる。上記実施の形態における未知攻撃の判定は、HTTPに限らず、インターネットの様々な通信プロトコルでも同様に適用できる。インターネットにおける通信プロトコルは、予め規定される予約語によって識別されるTLV(Type Length Value)

10

20

30

40

50

length Value) と、その値との組み合わせにより表現され、プロトコルサーバに送信する例が多い。これは、Webサーバにおいて取り扱うCGIに類似し、プロトコルサーバへの攻撃手法も、Webサーバへの攻撃手法と類似するので、前述する実施の形態と同様に未知攻撃の可能性を判定する。

【0080】

具体的には、電子メールの送信や中継を行うSMTP (Simple Mail Transfer Protocol) やFTPでは、「コマンド」として規定されているTLVの変数の値が長い値で与えられた場合、SMTPサーバやFTPサーバがバッファオーバーフローしてしまう攻撃が数多く存在する。また、DNS (Domain Name System) において「クエリ」と規定されているTLVについても同様である。

10

【0081】

さらに、BGP (Border Gateway Protocol) やOSPF (Open Shortest Path First) といったルーティングプロトコルの分野では、ベンダー (Vendor) が製品開発のために自由に定義できるTLVを許している例が多い。このことは、ベンダーが未定義のTLVに値を入れるだけで、当該ベンダーのプロトコルサーバがクラッシュしてしまう攻撃も存在する。よって、TLV形式を用いたアプリケーションのプロトコルサーバに対する未知攻撃を判定するために、上記実施の形態で説明したWebサーバを対象とした場合の未知攻撃判定方法を適用すれば、有効な解決手段となりうるものである。

【0082】

また、各実施の形態は可能な限り組み合わせることで実施することが可能であり、その場合には組み合わせによる効果が得られる。さらに、上記各実施の形態には種々の上位、下位段階の発明が含まれており、開示された複数の構成要素の適宜な組み合わせにより種々の発明が抽出され得るものである。例えば問題点を解決するための手段に記載される全構成要件から幾つかの構成要件が省略されうることによって発明が抽出された場合には、その抽出された発明を実施する場合には省略部分が周知慣用技術で適宜補われるものである。

20

【0083】

【発明の効果】

以上説明したように本発明によれば、未知の攻撃に対し、攻撃検知の正確性が完全でない場合でも、防御対象の正常なサービスを停止させず、当該防御対象の致命的な被害から守ることができるパケット転送システム、パケット転送装置、プログラム及びパケット転送方法を提供できる。

30

【図面の簡単な説明】

【図1】本発明の第1の実施の形態に係るパケット転送システム及びパケット転送装置を示す構成図。

【図2】図1に示すパケット転送装置によって複数の受信パケットから得られる通信アプリケーションデータの解析による統計的な評価値を説明する分布図。

【図3】本発明の第1の実施の形態に係るプログラム及びパケット転送方法を説明する機能ブロック図。

【図4】本発明の第1の実施の形態に係るプログラム及びパケット転送方法を説明する処理の流れ図。

40

【図5】パケット統計解析テーブル及びアノマリ型パケット転送テーブルのデータ配列図。

【図6】本発明の第2の実施の形態に係るパケット転送システム及びパケット転送装置を示す構成図。

【図7】図6に示すパケット転送装置によって複数の受信パケットから得られる通信アプリケーションデータの解析による統計的な評価値を説明する分布図。

【図8】アノマリ型パケット転送テーブルのデータ配列図。

【図9】本発明の第2実施の形態に係るプログラム及びパケット転送方法を説明する機能ブロック図。

50

【図10】本発明の第2の実施の形態に係るプログラム及びパケット転送方法を説明する処理の流れ図。

【図11】本発明の第3の実施の形態に係るパケット転送システムを示す構成図。

【図12】URLスイッチの負荷分散テーブルによる負荷の分散状態を説明する図。

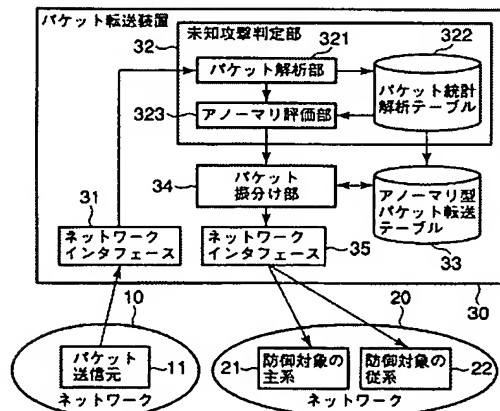
【図13】従来の通信アプリケーションデータの解析による統計的な評価値を説明する分布図。

【符号の説明】

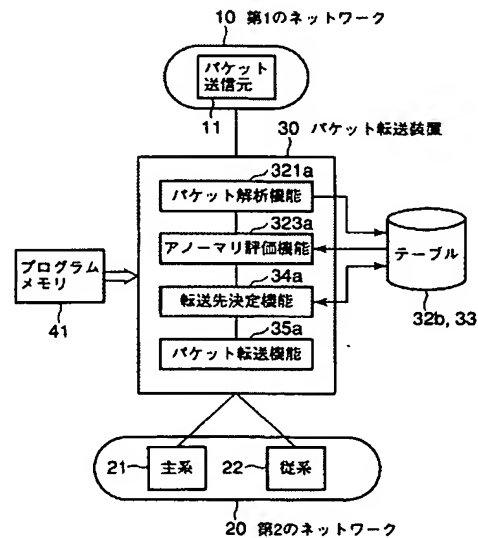
10…第1のネットワーク、11…パケット送信元、20…第2のネットワーク、21…防御対象の主系、22、221～22N…防御対象の従系、32…未知攻撃判定部、33…アノーマリ型パケット転送テーブル、34…パケット振分け部、34a…転送先決定機能、34b…従系攻撃検知識別機能、321…パケット解析部、321a…パケット解析機能、322…パケット統計解析テーブル、323…アノーマリ評価部、323a…アノーマリ評価機能、23、241～24N…ホスト型IDS、35a…パケット転送機能、35b…従系切替機能。

10

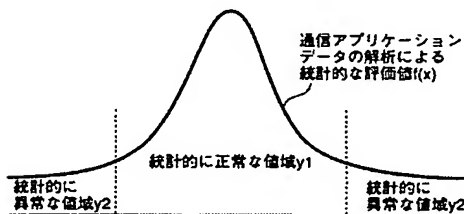
【図1】



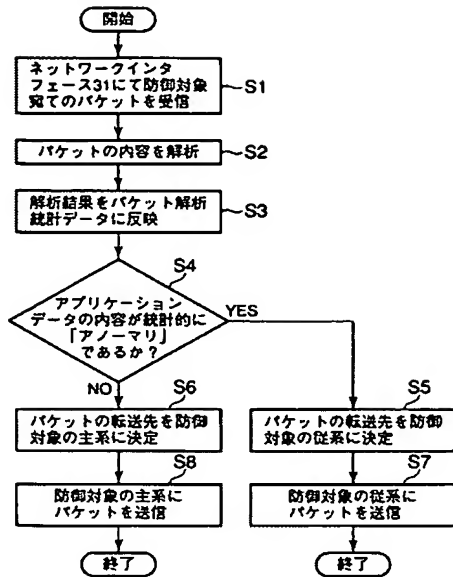
【図3】



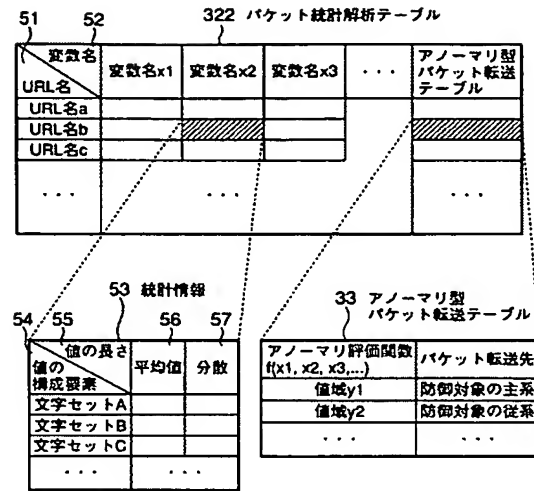
【図2】



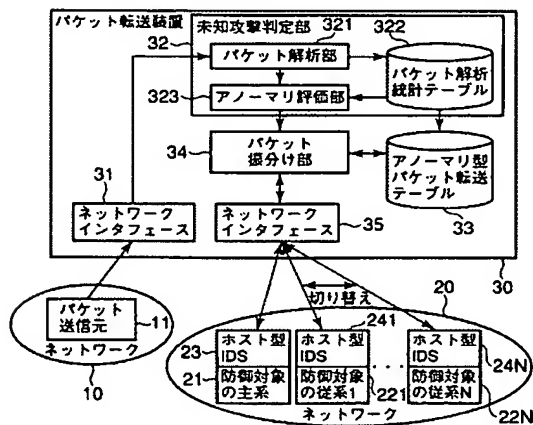
【図4】



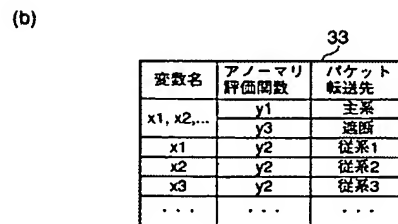
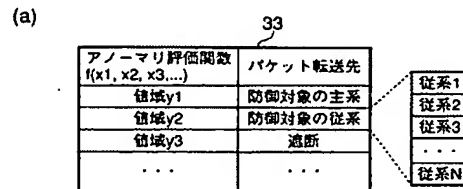
【図5】



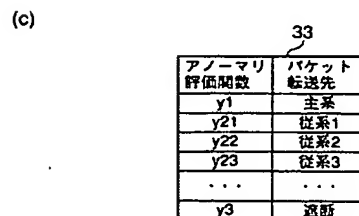
【図6】



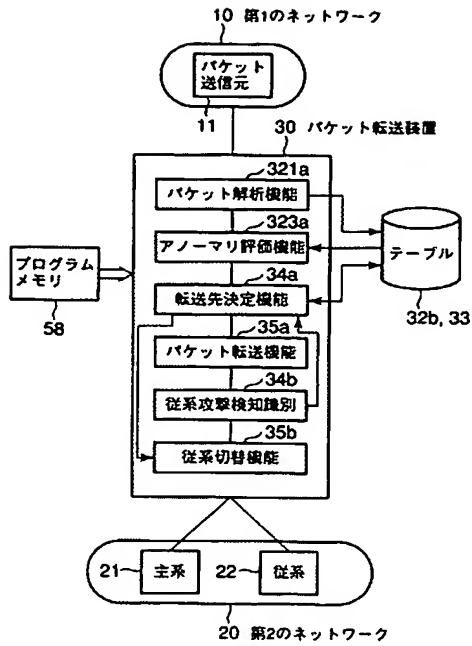
【図8】



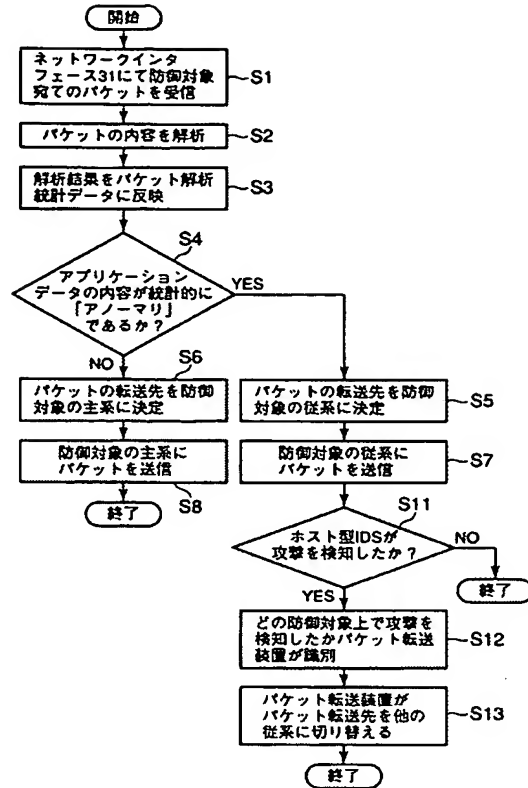
【図7】



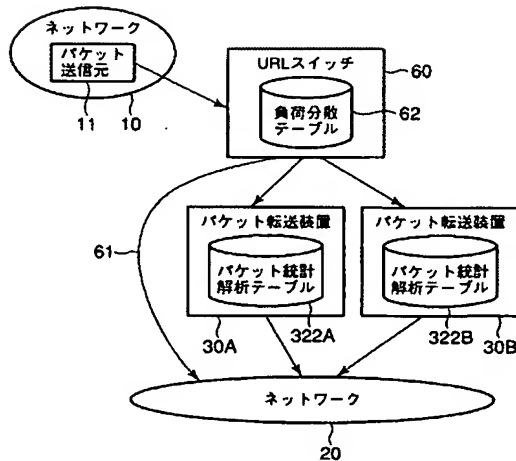
【図 9】



【図 10】



【図 11】



【図 12】

(a)

URLスイッチの
負荷分散テーブル

URL名	負荷分散先
URL名a	30A
URL名b	30A
URL名c	30A
URL名d	30B
URL名e	30B
URL名f	30B
URL名g	20
URL名h	20
URL名i	20
...	...

(b)

322A

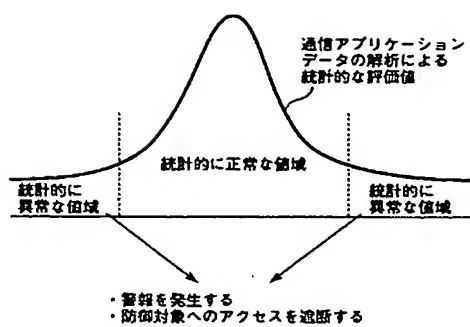
変数名	変数名x1	変数名x2	変数名x3	...	アノマリ型 パケット転送 テーブル
URL名					
URL名a					
URL名b					
URL名c					
...

(c)

322B

変数名	変数名x1	変数名x2	変数名x3	...	アノマリ型 パケット転送 テーブル
URL名					
URL名d					
URL名e					
URL名f					
...

【図 13】



フロントページの続き

(72)発明者 今野 徹

東京都府中市東芝町1番地 株式会社東芝府中事業所内

Fターム(参考) 5K030 GA15 HB16 HD06 KA07 LB08

5K033 AA08 CB08 DA06 DB18